

CLAIMS

1. A file security system for restricting access to electronic files, said file security
5 system comprising:

a key store that stores a plurality of cryptographic key pairs, each of the
cryptographic key pairs includes a public key and a private key, at least one of the
cryptographic key pairs pertaining to a predetermined time; and

an access manager operatively connected to said key store, said access
10 manager determines whether the private key of the at least one of the cryptographic
key pairs pertaining to the predetermined time is permitted to be provided to a
requestor based on a current time,

wherein the requestor requires the private key of the at least one of the
cryptographic key pairs pertaining to the predetermined time to access a secured
15 electronic file, and wherein the secured electronic file was previously secured using
the public key of the at least one of the cryptographic key pairs pertaining to the
predetermined time.

2. A file security system as recited in claim 1, wherein said access manager only
20 provides the private key of the at least one of the cryptographic key pairs pertaining
to the predetermined time to the requestor if the predetermined time is greater than
or equal to the current time.

3. A file security system as recited in claim 1, wherein the requestor is a client
25 module that operatively connects to said access manager over a network.

4. A file security system as recited in claim 1, wherein said document security
system further comprises:

at least one client module, said client module assists a user in selecting the
30 predetermined time, and said client module secures the electronic file using the

public key of the at least one of the cryptographic key pairs pertaining to the predetermined time so as to provide a time-based access restriction to the electronic file.

5 5. A file security system as recited in claim 4, wherein said client module further assists in unsecuring the secured electronic file by acquiring the private key of the at least one of the cryptographic key pairs that pertaining to the predetermined time from said key store, and then unsecuring the secured electronic file using the private key of the at least one of the cryptographic key pairs that pertaining to the
10 predetermined time.

6. A method for restricting access to an electronic document, said method comprising:
identifying an electronic document to be secured, the electronic document
15 having at least a data portion that contains data;
obtaining a time-based access key;
securing the electronic document through use of the time-based access key to produce a secured electronic document; and
storing the secured electronic document.

20

7. A method as recited in claim 6, wherein the time-based access key has an access time associated therewith.

8. A method as recited in claim 7,
25 wherein said method further comprises:
storing the time-based access key at a remote key store, and
wherein the time-based access key is subsequently retrievable from the remote key store only if the current time equals or exceeds the access time associated with the time-based access key.

9. A method as recited in claim 8, wherein said method is performed on a client machine that operatively receives the time-based access key from the remote key store over a network.

5

10. A method for restricting access to an electronic document, said method comprising:

identifying an electronic document to be secured, the electronic document having at least a data portion that contains data;

10 obtaining a document key;

encrypting the data portion of the electronic document using the document key to produce an encrypted data portion;

obtaining a time-based access key;

15 encrypting the document key using the time-based access key to produce an encrypted document key;

forming a secured electronic document from at least the encrypted data portion and the encrypted document key; and

storing the secured electronic document.

20 11. A method as recited in claim 10, wherein the time-based access key is a public time-based access key.

12. A method as recited in claim 10, wherein the time-based access key has an access time associated therewith.

25

13. A method as recited in claim 12, wherein the time-based access key is available from a remote key store only if the current time equals or exceeds the access time associated with the time-based access key.

14. A method as recited in claim 13, wherein the access time is a day of a year, and the time-based access keys are unique for each day of the year.

15. A method as recited in claim 13, wherein said method is performed on a client machine that operatively receives the time-based access key from the remote key store over a network.

16. A method for accessing a secured electronic document by a requestor, the secured electronic document having at least a header portion and a data portion, said method comprising:

obtaining a time-based access key;

obtaining an encrypted document key from the header portion of the secured electronic document;

decrypting the encrypted document key using the time-based access key to produce a document key;

decrypting an encrypted data portion of the secured electronic document using the document key to produce a data portion; and

supplying the data portion to the requestor.

17. A method as recited in claim 16, wherein the time-based access key is identified by an indicator within a header portion of the secured electronic document.

18. A method as recited in claim 16, wherein the time-based access key is a private time-based access key.

19. A method as recited in claim 18, wherein the time-based access key being obtained is acquired from a server.

20. A method as recited in claim 16, wherein said obtaining of the time-based access key is dependent on the current time.

21. A method as recited in claim 16, wherein the time-based access key is
5 associated with an access time, and wherein said obtaining of the time-based access key is permitted only when the current time is greater than or equal to the access time.

22. A method as recited in claim 21, wherein, if permitted, said obtaining obtains
10 the time-based access key being obtained from a server.

23. A method for distributing cryptographic keys used in a file security system, said method comprising:

receiving a request for a time-based key;

15 identifying an access time associated with the time-based key;

comparing the current time with the access time; and

refusing to distribute the time-based key in response to the request when said
comparing indicates that the current time is prior to the access time.

20 24. A method as recited in claim 23, wherein the time-based key is a private time-based key.

25 25. A method as recited in claim 23, wherein said method is performed at a server, and wherein the request for the time-based key is from a client module that is connectable to the server via a network.

26. A computer readable medium including at least computer program code for restricting access to an electronic document, said computer readable medium comprising:

computer program code for identifying an electronic document to be secured,
5 the electronic document having at least a data portion that contains data;

computer program code for obtaining a time-based access key;

computer program code for securing the electronic document through use of the time-based access key to produce a secured electronic document; and

computer program code for storing the secured electronic document.

10

27. A computer readable medium as recited in claim 26, wherein the time-based access key has an access time associated therewith.

28. A computer readable medium as recited in claim 27,

15 wherein said computer readable medium further comprises:

computer program code for storing the time-based access key at a remote key store, and

wherein the time-based access key is subsequently retrievable from the remote key store only if the current time equals or exceeds the access time
20 associated with the time-based access key.